

## FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 01/03/2006

To: San Francisco

From: San Francisco

Squad 14G/SJRA

Contact: SA [REDACTED]

Approved By: [REDACTED] *maj/L*

Drafted By: [REDACTED] *dm*

Case ID #: 288A-SF-NEW (Pending)

Title: UNSUB(s);  
~~SANTY WORM~~  
GOOGLE INC. - VICTIM

Synopsis: To open and assign a new case on the Santy worm.

Details: On December 22, 2005, [REDACTED] Google Inc., reported Google search engine queries originating from computers compromised by the Santy worm was affecting performance of their website. [REDACTED] further described the direct effects and damages to Google caused by the different variants of the Santy worm. The Santy worm, written in Perl script language, exploits a vulnerability in the phpBB bulletin board/web forum software to spread and it uses the Google search engine to find additional vulnerable servers running phpBB software. This worm has been plaguing Google for the last 12-18 months as Google has attempted to filter out the search requests caused by the worm. As Google filters out certain string search phrases, within minutes, the subjects modify the search phrase to once again, bypass Google's filters. Unfortunately, because the worm is attempting to propagate using the Google search engine, Google is beginning to block many legitimate requests to the Google search engine.

Currently, Google has an engineering team devoted to blocking the variants of the worm. Google preliminarily estimated that it has sustained approximately \$250,000 - 500,000 in damages just trying to control the spread of the worm. This loss calculation is based on man hours dedicated to the problem in addition to lost revenues.

Google engineers have analyzed the script from one flavor of the Santy worm and discovered gmail addresses for a technical contact posted in the comment section of the script. This may be the email address of the creator of that particular variant of

Open

288A-SF-139138-01

To: San Francisco From: San Francisco  
Re: 288A-SF-NEW, 01/03/2006

b6  
b7C

the worm. The following gmail addresses were found in the script: [redacted] and [redacted]

It is recommended that a new case be opened and assigned to SA's [redacted] and [redacted] as co-case agents.

♦♦

# United States District Court

NORTHERN

DISTRICT OF CALIFORNIA

TO:



## SUBPOENA TO TESTIFY BEFORE GRAND JURY

b3

SUBPOENA FOR:

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 07-06-2009 BY 60322/UC/LRP/PLJ/sdb

☐ PERSON ☒ DOCUMENT(S) OR OBJECT(S)

YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specified below.

<b>PLACE</b> United States District Court United States Courthouse 280 South First Street San Jose, CA 95113	<b>COURTROOM</b> As directed by the court <hr/> <b>DATE AND TIME</b> January 18, 2006 at 9:30am
--	--

YOU ARE ALSO COMMANDED to bring with you the following document(s) or object(s):\*

-SEE ATTACHMENT-

COMPLIANCE WITH THE SUBPOENA WILL BE DEEMED SATISFACTORY WHEN YOU PROVIDE ALL THE REQUIRED MATERIALS TO THE AGENT SERVING THIS SUBPOENA AND NO APPEARANCE WILL BE NECESSARY.

☒ Please see additional information on reverse

This subpoena shall remain in effect until you are granted leave to depart by the court or by an officer acting on behalf of the court

U.S. MAGISTRATE JUDGE OR CLERK OF COURT

**RICHARD W. WIEKING**

(By) Deputy Clerk

*Richard W. Wieking*



DATE

*[Signature]*  
January 4, 2006

This subpoena is issued on application  
of the United States of America  
KEVIN V. RYAN  
United States Attorney

ATTORNEY'S ADDRESS AND PHONE NUMBER:  
AUSA, MATTHEW A. PARRELLA  
U.S. Attorney's Office, 150 Almaden Blvd., Suite 900  
San Jose, CA 95113 (408)535-5061  
Special Agent Dana Marino, FBI (408) 535-4685

\*If not applicable, enter "none"

✓ 288A-SF/39138-2



U.S. Department of Justice

b3

United States Attorney  
Northern District of California

150 Almaden Boulevard, Suite 900  
San Jose, California 95113

DD: (408) 535-5061  
FAX: (408) 535-5066

January 4, 2006

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 07-06-2009 BY 60322/UC/LRP/PLJ/sdb

Re: Grand Jury Investigation  
Request for Non-Disclosure

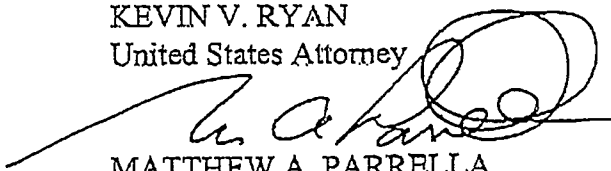
Dear Custodian of Records:

Pursuant to an investigation being conducted by the Federal Grand Jury for the Northern District of California with regard to possible felony violations of the United States Code, it is requested that you furnish the information requested in the grand jury subpoena.

In addition, we request that you not disclose the existence of this request and the production of records. Any such disclosure could impede the investigation being conducted and thereby interfere with the enforcement of the law. Thank you very much for your assistance in this matter.

Very truly yours,

KEVIN V. RYAN  
United States Attorney

  
MATTHEW A. PARRELLA  
Assistant United States Attorney

MAP: lg

RETURN OF SERVICE<sup>1</sup>

RECEIVED BY SERVER	DATE 1/4/2006	PLACE San Jose, CA
SERVED	DATE 1/4/2006	PLACE Mountain View, CA

SERVED ON (PRINT NAME)

SERVED BY (PRINT NAME)

TITLE

Special Agent

## STATEMENT OF SERVICE FEES

TRAVEL	SERVICES	TOTAL
--------	----------	-------

DECLARATION OF SERVER<sup>2</sup>

I declare under penalty of perjury under the laws of the United States of America that the foregoing information contained in the Return of Service and Statement of Service Fees is true and correct.

Executed on 1/4/2006  
Date

Signature of Server

FBI, 900 S Bascom Ave, ST, CA  
Address of Server

## Additional Information

Note: Served via facsimile

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 07-06-2009 BY 60322/UC/LRP/PLJ/sdb

<sup>1</sup>As to who may serve a subpoena and the manner of its service see Rule 17(d), Federal Rules of Criminal Procedure, or Rule 45(c), Federal Rules of Civil Procedure.

<sup>2</sup>"Fees and mileage need not be tendered to the witness upon service of a subpoena issued on behalf of the United States or an officer or agency thereof (Rule 45(c), Federal Rules of Civil Procedure; Rule 17(d), Federal Rules of Criminal Procedure) or on behalf of certain indigent parties and criminal defendants who are unable to pay such costs (28 USC 1825, Rules 17(b) Federal Rules of Criminal Procedure)".

(Rev. 01-31-2003)

b6  
b7c

## FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 01/31/2006

To: San Francisco

From: San Francisco  
Squad 14G/ SJRA  
Contact: SA [REDACTED]

Approved By: [REDACTED] JrM1

Drafted By: [REDACTED]: dm Dm

Case ID #: ✓288A-SF-139138-5 (Closed)

Title: UNSUB(s);  
SANTY WORM;  
GOOGLE INC. - VICTIM

**Synopsis:** Google is not interested in pursuing this matter. It is recommended this case be closed.

**Details:** On January 30, 2006, [REDACTED] Google Inc., advised that the legal department of Google is not interested in conducting any further investigation into this matter.

Inasmuch as Google is the victim and their assistance in the form of providing logs and other supporting documentation is necessary to pursue prosecution, it is recommended this case be administratively closed.

♦♦

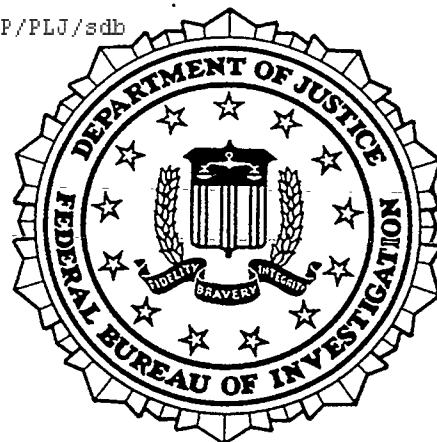
<b>SF Field Intelligence Group</b>	
Potential Intel Value: Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>	
Reviewed By: <u>MA</u>	Date: <u>2/7/06</u>
S-Drive Location: _____	

Close (4)

MA 2/7/06  
Case closed 2/7/06  
DGS

Close

# *San Francisco FBI Cyber Squad 14G*



## *Facsimile Coversheet*

Fax Date: 1/4/06  
Fax Time: \_\_\_\_\_

Number of Pages: 4  
(including cover page)

**To:**

b3

**Recipient's Fax Number:**

**Subject:** *This subpoena is related to the one  
Sent yesterday.*

b6  
b7C

**From:** *Special Agent*

*Federal Bureau of Investigation  
950 South Bascom Avenue, Suite 3011  
San Jose, California 95128*

# United States District Court

NORTHERN

DISTRICT OF CALIFORNIA

TO:



## SUBPOENA TO TESTIFY BEFORE GRAND JURY

b3

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 07-06-2009 BY 60322/UC/LRP/PLJ/sdb

SUBPOENA FOR:

☐ PERSON ☒ DOCUMENT(S) OR OBJECT(S)

YOU ARE HEREBY COMMANDED to appear and testify before the Grand Jury of the United States District Court at the place, date, and time specified below.

PLACE

United States District Court  
United States Courthouse  
280 South First Street  
San Jose, CA 95113

COURTROOM

As directed by the court

DATE AND TIME

January 11, 2006 at 9:30am

YOU ARE ALSO COMMANDED to bring with you the following document(s) or object(s):\*

-SEE ATTACHMENT-

COMPLAINE WITH THE SUBPOENA WILL BE DEEMED SATISFACTORY WHEN YOU PROVIDE ALL THE REQUIRED MATERIALS TO THE AGENT SERVING THIS SUBPOENA AND NO APPEARANCE WILL BE NECESSARY.

☒ Please see additional information on reverse

This subpoena shall remain in effect until you are granted leave to depart by the court or by an officer acting on behalf of the court

U.S. MAGISTRATE JUDGE OR CLERK OF COURT

**RICHARD W. WIEKING**

(By) Deputy Clerk

DATE

December 28, 2005

This subpoena is issued on application  
of the United States of America  
KEVIN V. RYAN  
United States Attorney

ATTORNEY'S NAME, ADDRESS AND PHONE NUMBER:

AUSA, MATTHEW A. PARRELLA  
U.S. Attorney's Office, 150 Almaden Blvd., Suite 900  
San Jose, CA 95113 (408)535-5061  
Special Agent Dana Marino, FBI (408) 535-4685

\*If not applicable, enter "none"

✓ 288A-SF-139138-3





U.S. Department of Justice

United States Attorney  
Northern District of California

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 07-06-2009 BY 60322/UC/LRP/PLJ/sdb

150 Almaden Boulevard, Suite 900  
San Jose, California 95113

DD: (408) 535-5061  
FAX: (408) 535-5066

December 28, 2005



b3

Re: Grand Jury Investigation  
Request for Non-Disclosure

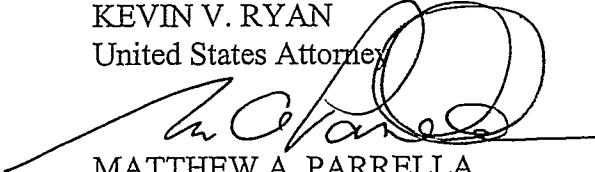
Dear Custodian of Records:

Pursuant to an investigation being conducted by the Federal Grand Jury for the Northern District of California with regard to possible felony violations of the United States Code, it is requested that you furnish the information requested in the grand jury subpoena.

In addition, we request that you not disclose the existence of this request and the production of records. Any such disclosure could impede the investigation being conducted and thereby interfere with the enforcement of the law. Thank you very much for your assistance in this matter.

Very truly yours,

KEVIN V. RYAN  
United States Attorney

  
MATTHEW A. PARRELLA  
Assistant United States Attorney

MAP: lg

RETURN OF SERVICE<sup>1</sup>

RECEIVED BY SERVER	DATE 1/3/06	PLACE San Jose, CA
SERVED	DATE 1/3/06	PLACE Mountain View, CA
SERVED ON (PRINT NAME)		
SERVED BY (PRINT NAME)	TITLE Special Agent	

b3  
b6  
b7C

## STATEMENT OF SERVICE FEES

TRAVEL	SERVICES	TOTAL

b6  
b7CDECLARATION OF SERVER<sup>2</sup>

I declare under penalty of perjury under the laws of the United States of America that the foregoing information contained in the Return of Service and Statement of Service Fees is true and correct.

Executed on 1/3/2006  
Date

Signature of Server

FBI 950 S. Bascom, SJ, CA  
Address of Server

## Additional Information

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 07-06-2009 BY 60322/UC/LRP/PLJ/sdb

<sup>1</sup> As to who may serve a subpoena and the manner of its service see Rule 17(d), Federal Rules of Criminal Procedure, or Rule 45(c), Federal Rules of Civil Procedure.

<sup>2</sup> "Fees and mileage need not be tendered to the witness upon service of a subpoena issued on behalf of the United States or an officer or agency thereof (Rule 45(c), Federal Rules of Civil Procedure; Rule 17(d), Federal Rules of Criminal Procedure) or on behalf of certain indigent parties and criminal defendants who are unable to pay such costs (28 USC 1825, Rules 17(b) Federal Rules of Criminal Procedure)".

HP OfficeJet K Series K80xi  
Personal Printer/Fax/Copier/Scanner

Log for  
HT Internet

b6  
b7c

Jan 04 2006 4:26pm

---

Last Transaction

<u>Date</u>	<u>Time</u>	<u>Type</u>	<u>Identification</u>	<u>Duration</u>	<u>Pages</u>	<u>Result</u>
Jan 4	4:24pm	Fax Sent		2:08	4	OK

---

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 07-06-2009 BY 60322/UC/LRP/PLJ/sdb